



# **Performance Audit Mobile Device Security Risks**

November 2016



**Office of the City Auditor**

**City of Kansas City, Missouri**

12-2016





## Office of the City Auditor

21<sup>st</sup> Floor, City Hall  
414 East 12<sup>th</sup> Street  
Kansas City, Missouri 64106

(816) 513-3300  
Fax: (816) 513-3305

November 2, 2016

Honorable Mayor and Members of the City Council:

This performance audit focuses on determining whether the city has taken adequate steps to mitigate security risks related to smartphones and tablets used for city business.

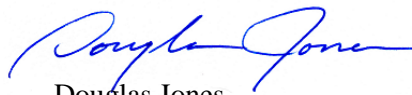
Mobile devices are portable computing devices such as smartphones and tablets that allow users to access data, email, the Internet, GPS navigation, and other applications remotely. Security measures, such as firewalls, antivirus software, and encryption, are uncommon on mobile devices, and mobile device operating systems are not updated as frequently as those on personal computers and laptops, making them more susceptible to cyberattacks.

Although the city has some mobile device security policies, it lacks some critical safeguards that mitigate mobile device security vulnerabilities. Furthermore, city policies require some key security features to be implemented on users' mobile devices, but they are not followed by all city smartphone and tablet users.

Mobile devices are subject to numerous security threats. Any mobile device with unimplemented security safeguards leaves a hole in the city's defense against unauthorized access to city data or can lead to harm to the city's information systems. Using mobile device management software can enforce key security requirements and protect the city's information systems and data.

We make recommendations to ensure city data accessed by, and stored on mobile devices is more protected, mobile device security requirements are followed; and mobile device users understand the importance of mobile device security requirements and how to implement them.

The draft report was sent to the director of general services and the chief information officer on September 29, 2016, for review and comment. Management's response is appended. We would like to thank the General Services Department's Information Technology Division staff for their assistance and cooperation during this audit. We also want to thank the city employees who completed the mobile device survey. The audit team for this project was Sue Polys and Vivien Zhi.

  
Douglas Jones  
City Auditor



---

# Mobile Device Security Risks

---

## Table of Contents

---

<b>Introduction</b>	1
Objectives	1
Scope and Methodology	1
Mobile Device User Survey	2
Review of Security Features on Mobile Devices	2
Background	3
Mobile Device Security Vulnerabilities	3
Mobile Devices Used for City Business	3
<b>Findings and Recommendations</b>	5
Summary	5
City Policies Do Not Address Some Mobile Device Security Risks	5
City Should Require Operating System Updates	6
City Should Require Location Services Be Disabled When Not in Use	6
City Should Require Immediate Reporting of Lost Devices to IT	7
City Should Require Safe Syncing and Backup	8
City Should Require Surface Tablets Be Encrypted	8
Required Key Security Features Are Not Consistently Used	9
Not All City Mobile Devices Require a Passcode	9
Mobile Device Bluetooth Functionality Not Always Disabled When Not in Use	10
City Should Provide More Directions on Downloading Apps to Mobile Devices	10
Mobile Device Security Training Can Enhance Security	11
Mobile Device Management Software Can Enforce Key Security Features	11
Recommendations	13
<b>Appendix A</b>	15
Director of General Services' Response	15



---

## Introduction

---

### Objectives

We conducted this audit of mobile device security risks under the authority of Article II, Section 216 of the Charter of Kansas City, Missouri, which establishes the Office of the City Auditor and outlines the city auditor's primary duties.

A performance audit provides "findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability."<sup>1</sup>

This report is designed to answer the following question:

- Has the city taken adequate steps to mitigate security risks related to smartphones and tablets used for city business?

---

### Scope and Methodology

Our review focuses on reviewing security practices on smartphones and tablets that are used for city business. Our audit methods included:

- Surveying smartphone and tablet users that use the devices for city business to understand employees' knowledge of the city's mobile security policies; to determine what security practices employees have implemented on their mobile devices; and to identify instructions received from the city about mobile device security responsibilities.

---

<sup>1</sup> Comptroller General of the United States, *Government Auditing Standards* (Washington, DC: U.S. Government Printing Office, 2011), p. 17.

- Comparing city policies and recommended mobile device security practices to survey responses to identify gaps between users' practices and city policies and recommended practices.
- Reviewing the security features on a sample of selected smartphones and tablets to determine whether the devices comply with city policies and recommended practices related to mobile device security.
- Reviewing *Administrative Regulation 1-16*, "Technology Procurement, Use and Security" and *Bring Your Own Device (BYOD) Acceptable Use and Stipend or Deduction* policy to identify the city's security requirements related to mobile devices.
- Reviewing the National Institute of Standards and Technology's (NIST) *Guidelines for Managing the Security of Mobile Devices in the Enterprise* to identify criteria and recommended practices related to managing the security of mobile devices.
- Interviewing fiscal officers, Information Technology (IT) staff, and smartphone and tablet users to understand how the city administers and manages mobile devices.

### **Mobile Device User Survey**

On June 7, 2016, we emailed a survey to 629 smartphone and tablet users who are either using a city-owned smartphone or tablet or using a personal phone for city business. The survey asked questions about user's knowledge of the city's mobile device security policies, security practices implemented on their smartphones or tablet, and instructions they received from the city about mobile device security responsibilities. The survey was closed on June 17, 2016. We received 328 responses for a response rate of 52 percent.

### **Review of Security Features on Mobile Devices**

We judgmentally selected twenty-three mobile devices to review their security features. We selected fourteen city-owned devices that can be only used for city business, including two Surface tablets, four iPads, and eight cellphones; five city-owned cellphones that can be used for personal use; and four personally owned cellphones that employees can use for work. We examined the security features on the devices against a set of examination criteria that was developed based on recommended mobile device security practices and city policies.



We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. No information was omitted from this report because it was deemed privileged or confidential.

---

## Background

### Mobile Device Security Vulnerabilities

Mobile devices are portable computing devices that allow users to access data, email, the Internet, GPS navigation, and other applications remotely. Although mobile devices may improve productivity, they also expose the city to new security risks, such as downloading malware<sup>2</sup> to the city's devices and network or exposing confidential information. Security measures, such as firewalls, antivirus software, and encryption, are uncommon on mobile devices, and mobile device operating systems are not updated as frequently as those on personal computers and laptops, making them more susceptible to cyberattacks. Security threats to mobile devices also include loss or theft, unauthorized access to networks or data, and the ability to identify user location.

### Mobile Devices Used for City Business

The city owns over 750 smartphones and tablets used by employees for city business. The city's bring your own device (BYOD) policy permits two options for employees who need a cellphone for city business and want to use it for personal use. The first option allows employees to use a city-owned cellphone and pay a portion of the usage cost. As of May 2016, there were 123 employees choosing this option. The second option allows employees to use their personal cellphone and receive a stipend to defray the cost of using it for city business. As of May 2016, there were 226 employees using this option.

---

<sup>2</sup> Malware is software used to disrupt computer operations, gather sensitive information, gain access to computer systems, or display unwanted advertising. Malware includes viruses, Trojan horses, ransomware, spyware, and other malicious programs.



---

## Findings and Recommendations

---

### Summary

Mobile devices are subject to numerous security threats. Although the city has some mobile device security policies, it lacks some critical requirements to mitigate mobile device security vulnerabilities, including requiring operating system updates, location services to be disabled when not in use, immediate reporting of lost devices to the Information Technology Division (ITD), safeguards for syncing and backup of mobile devices used for city business, and requiring encryption on data stored on Surface tablets. The city should update the city's mobile device security policies to help ensure the risks are mitigated.

Although city policies require some key security features to be implemented on users' mobile devices, not all city smartphone and tablet users are following them. Not all mobile devices used for city business require a passcode to access; users are not disabling Bluetooth functionality when the function is not in use; and the city has not provided adequate instructions on downloading apps. The city should require users to receive mobile device security training to ensure the users understand the importance of mobile device security requirements and how to follow the requirements.

Any mobile device with unimplemented security safeguards leaves a hole in the city's defense against unauthorized access to city data or can lead to harm to the city's information systems. The city should implement mobile device management software on mobile devices used for city business to enforce key security requirements.

---

### City Policies Do Not Address Some Mobile Device Security Risks

Mobile devices are subject to numerous security vulnerabilities. Although the city has some mobile device security policies, it lacks some critical safeguards that would mitigate mobile device security vulnerabilities, including operating system updates; location services disabled when not in use; immediate reporting of lost devices to ITD; safeguards for syncing and backup of mobile devices used for city business; and encryption of data stored on Surface tablets. To ensure the

vulnerabilities are mitigated, the chief information officer should update the city's mobile device security policy.

### **City Should Require Operating System Updates**

*Administrative Regulation (AR) 1-16*<sup>3</sup>, which addresses mobile device security, does not require the most current operating systems to be installed on mobile devices. Mobile device security recommended practices suggest updating operating systems as soon as updates are released. Security notifications about new vulnerabilities occur on a regular basis. Some vulnerabilities allow attackers to steal users' login information, or execute malicious code. To combat these issues, software companies release security patches in newer versions of operating systems. Users need to keep the device software current to protect it from vulnerabilities.

We surveyed city mobile device users about how security practices are implemented on their smartphones or tablets. About 29 percent of the smartphone respondents and 55 percent of the tablet respondents said they do not have the most current operating system installed on their devices. While examining devices, we found eight out of 23 devices did not have the most current version of the operating system installed. Installing the most current operating system update ensures devices have the security patches needed to remediate the latest discoveries of system errors or vulnerabilities so malicious hackers cannot take advantage of operating system flaws. If a user's mobile device does not have the most current version of the operating system, malicious attackers can steal confidential information and gain unauthorized access to the city's information systems.

To ensure the most current security patches are installed on mobile devices, the chief information officer should revise *AR 1-16* to require users to update the operating system on their mobile devices used for city business to the most current version.

### **City Should Require Location Services Be Disabled When Not in Use**

City policy does not require employees to disable location services on mobile devices when not in use. Location services are used by social media, navigation, web browsers, and other mobile applications to determine the user's location. According to mobile device security recommended practices, location services should be disabled when not in use to reduce the risk of targeted attacks. Location services detect a device's physical location. Potential attackers can determine where a

---

<sup>3</sup> *Administrative Regulation No. 1-16*, "Technology Procurement, Use, and Security," July 2015.

user and mobile device are when location services are enabled. Attackers can target the device with phishing<sup>4</sup> and other social engineering<sup>5</sup> attacks in order to steal information. In our mobile device user survey, about 67 percent of smartphone respondents and 71 percent of tablet respondents stated that they do not disable location services when not in use.

To minimize the risk that users' location data will be tracked for malicious purposes, the chief information officer should revise *AR 1-16* to require users to disable location services on their mobile devices used for city business when not in use.

### **City Should Require Immediate Reporting of Lost Devices to IT**

*AR 1-16* covering both city and personal mobile devices used for city business does not require users to report lost or stolen devices immediately to IT. According to mobile device security recommended practices, organizations should have a policy on timely reporting of lost or stolen devices. The city's BYOD policy does require users to report lost or stolen smartphones to their supervisors, mobile device service providers, and IT as soon as possible.<sup>6</sup> However, this provision only applies to the BYOD cellphones. Employees using city phones only for city business are not required by *AR 1-16* to report lost phones immediately. Although *AR 7-1*<sup>7</sup> requires employees to report the loss or theft of city property to citywide security, there is no policy on reporting the loss or theft of a mobile device to IT immediately. If a mobile device is lost or stolen, it is at a higher risk of having its data accessed by an unauthorized user. If the incident is reported to IT immediately, IT can remotely wipe the city data from the lost or stolen phone quickly so the information stored on or accessed by the device will not be compromised.

To ensure remote wipes are performed timely and unauthorized access to city data is prevented, the chief information officer should revise *AR 1-16* to require users of all mobile devices used for city business to report lost or stolen devices to their supervisor and ITD immediately.

---

<sup>4</sup> Phishing is a social engineering attack that uses email or malicious websites to solicit personal information or system credentials by posing as a trustworthy organization.

<sup>5</sup> Social engineering is an attack to entice information system users and administrators into revealing sensitive and confidential information.

<sup>6</sup> *Bring Your Own Device (BYOD) Acceptable Use and Stipend or Deduction Policy*, May 2013.

<sup>7</sup> *Administrative Regulation No 7-1*, "Procedures for Reporting All City-Related Incidents, Accidents, or Thefts," February 2015.

### **City Should Require Safe Syncing and Backup**

*AR 1-16* does not require safeguards for syncing<sup>8</sup> and backing up mobile devices. According to mobile device security recommended practices, organizations should have policies on how and where to back up the organization's data and what information can be synced to other devices. For example, the policy should include whether an employee can sync or back up organizational data to a personal computer or remote data storage.<sup>9</sup> How mobile data is synced and backed up may impact data security and privacy. A mobile device connecting to a city computer can transmit malware to the city computer. Also, when a city mobile device is connected to a personal computer, or a city mobile device is connected to a remote backup service, the city's data is at risk of being stored in an unsecured location and accessible to unauthorized parties.

To ensure city data is stored at a secure location and city computers are not infected with malware, the chief information officer should revise *AR 1-16* to establish safeguards for safe syncing and backup of mobile devices used for city business.

### **City Should Require Surface Tablets Be Encrypted**

Not all Surface tablets owned by the city are encrypted to prevent unauthorized access to information. *AR 1-16* states that all confidential data must be encrypted and transported using secure technology, but the policy does not specifically spell out the requirements for smartphones and tablets. Mobile device security recommended practices state that data communications between the mobile devices and the organization's system, as well as stored data on both built-in storage and removable media storage should be encrypted. The city has at least 60 Surface tablets. One Surface tablet we examined did not appear to be encrypted. One city department that handles confidential information is still working on encrypting some of their Surface tablets.

The mobile nature of Surface tablets puts them at a higher risk of being lost or stolen. Some of the information stored on or accessed by city Surface tablets, such as health or tax records, may be confidential. If an unauthorized party obtained the devices, they could access confidential city information.

---

<sup>8</sup> Sync is short for synchronize. To sync is to connect a mobile device and a computer and update both with the most recent information.

<sup>9</sup> Remote backup storage is storage provided by remote or online backup services, such as iCloud, for backup, storage, and recovery of computer files.

To ensure city information stored on and accessed by the tablets will not be compromised and to protect confidential information, the chief information officer should revise *AR 1-16* to require encryption of all data stored on city Surface tablets.

---

## Required Key Security Features Are Not Consistently Used

City policies require some key security features to be implemented on users' mobile devices, but they are not followed by all city smartphone and tablet users. Not all mobile devices used for city business require a passcode; users are not disabling Bluetooth functionality when not in use; and the city has not provided adequate instructions on downloading apps. To ensure mobile device users understand the importance of mobile device security requirements and how to implement the requirements, the director of general services should ensure users receive mobile device security training.

### Not All City Mobile Devices Require a Passcode

Not all devices used for city business require a passcode to be entered before use as required by city policy. According to *AR 1-16*, "tablets or smartphones that have access to city information should have password/passcode protection functionality activated." The city's BYOD policy states that "any mobile phone that has data capabilities must be secured based on current security standards and policies, including password protection..."<sup>10</sup> The mobile nature of the devices makes them more likely to be lost or stolen so the data on the devices is at an increased risk of being compromised. If the device does not require authentication, unauthorized users could access sensitive information stored on or accessed by the mobile device. In our mobile device user survey, about 32 percent of smartphone respondents and 30 percent of tablet respondents stated their devices did not require a passcode to be entered before use. Two out of twenty-three mobile devices we examined did not have a passcode requirement. If a device that does not require a passcode gets into the hands of unauthorized parties, they can access the city's confidential information stored on or accessed by the mobile device.

---

<sup>10</sup> *Bring Your Own Device (BYOD) Acceptable Use and Stipend or Deduction Policy*, May 2013.

### **Mobile Device Bluetooth Functionality Not Always Disabled When Not in Use**

Users are not always disabling the Bluetooth<sup>11</sup> functionality on their mobile devices when they are not using the Bluetooth function. *AR 1-16* requires the Bluetooth functionality to be disabled when the function is not in use. In our mobile device user survey, about 53 percent of smartphone respondents and 58 percent of tablet respondents said that they do not disable the Bluetooth function on their devices when they are not using it. Thirteen out of 23 devices we examined had the Bluetooth function on when the users were not using the function. Bluetooth is considered a personal area network. Bluetooth-enabled devices are “visible” to other nearby devices when Bluetooth is turned on. Other nearby device users could access this private network and carry out attacks, such as denial of service, eavesdropping, etc. Unauthorized parties can steal sensitive information when the Bluetooth function is enabled.

### **City Should Provide More Directions on Downloading Apps to Mobile Devices**

City policy is not clear on the types of app stores employees should avoid. *AR 1-16* states “apps<sup>12</sup> added to your smartphone or tablet should be from a trusted app store or market.” However, the policy does not instruct users on what a trusted app store or market is. The city’s chief information security officer said that the intent of the *AR* is to try to keep employees away from foreign governments or dark web<sup>13</sup> types of stores where the chances of finding a deliberate, malicious app increases substantially. During our device examinations, most of the users said they downloaded apps from the Apple app store or the Google Play store. However, even the well-known app stores, such as Apple or Google Play, have had apps that turned out to be malicious. Users need to be educated on what to look for when downloading apps, such as who created the app, what it does, or what information it will access on the device. In our mobile device user survey, about 37 percent of the respondents said they do not check whether the apps request inappropriate permissions to the data on the devices or they do not know what it means. According to IT and recommended practices, users need to verify that apps only receive the necessary permission on the mobile

---

<sup>11</sup> Bluetooth is a wireless technology used for exchanging data over short distance from fixed and mobile devices, and building personal area networks.

<sup>12</sup> Apps are applications or software programs that can be downloaded on and accessed on smartphones or other mobile devices.

<sup>13</sup> Dark web is a collection of websites that use anonymity tools to hide their IP addresses. They are often used for criminal activities.



devices. If a user unknowingly downloaded a malicious app, the malware can allow an attacker to take control of the device. If a mobile device user's smartphone or tablet is infected with malware and the device is connected to a city computer, then the malware can infect the city's computer as well.

### **Mobile Device Security Training Can Enhance Security**

City employees using mobile devices for city business do not receive much security training. According to information technology recommended practices, a security training program is paramount to ensuring that people understand their IT security responsibilities and organizational policies, and how to properly use and protect the IT resources entrusted to them. In our mobile device user survey, only 28 percent of respondents said they received instructions from the city on device security features, such as passcodes, Bluetooth functionality, and location services, on their mobile devices. Failure to provide security training on mobile devices puts city data at risk. Although the city has some mobile device security policies, such as *AR 1-16* and the city's BYOD policy, users do not always implement them. Mobile device users need to be trained on how to set the security features on their devices and why these security settings are important to protect the mobile devices from unauthorized access.

To ensure mobile device users understand the importance of mobile device security requirements and how to implement the requirements, the director of general services should ensure users receive mobile device security training.

---

### **Mobile Device Management Software Can Enforce Key Security Features**

The city does not currently have mobile device management (MDM)<sup>14</sup> software to enforce key mobile data security features. According to mobile device security recommended practices, organizations should have MDM software installed on mobile devices to protect critical data. If the mobile device is owned by the organization, the MDM software manages the security of the entire device. If the device is owned by the employee but used for organization business, the MDM software typically manages security of applications related to organizational data only, not the entire device.

---

<sup>14</sup> Mobile Device Management (MDM) software is a type of security software used by an IT department to configure and secure mobile devices with access to the organization's IT systems.

MDM software can address some of the security risks we mentioned in previous sections of this report. It can ensure devices have the most current version of the operating system; require a passcode to access the device; and segregate personal and business data and apps. In addition, MDM software can perform remote wipes if the device is lost or stolen; encrypt data; inventory, install, update, and remove applications; monitor devices to determine whether security policies have been violated; and provide security reporting. Although the city has some mobile device security requirements, we determined they are not implemented consistently on devices. Any mobile device with unimplemented security safeguards leaves a hole in the city's defense against unauthorized access to city data or can lead to harm to the city's information systems. MDM software installed on a mobile device can enforce security requirements and suspend mobile device access when users do not implement required security features.

Although MDM software has a cost, a data breach can be more costly. According to ITD, a MDM license costs about \$5 per device per month. The city currently has about 980<sup>15</sup> smartphones and tablets used for city business. The monthly cost for the MDM software license for these devices would be around \$4,900. According to a Ponemon Institute study, it costs \$21,042 on average *per* compromised mobile device for an organization to investigate, contain, and remediate an attack, and at any point in time, 1.2 percent of employees' mobile devices are compromised.<sup>16</sup> As employees use mobile devices for an increasing number of activities and often store confidential data on the devices, mobile devices are under increasing cyber-attacks. Implementing MDM software should be more cost effective than addressing the costs related to a successful mobile device related cyber-attack.

To ensure city data accessed by mobile devices is more protected and security requirements are enforced, the director of general services should implement mobile device management software on mobile devices used for city business.

---

<sup>15</sup> There are about 750 city-owned smartphones and tablets and 230 personally owned smartphones that are used for city business.

<sup>16</sup> "*The Economic Risk of Confidential Data on Mobile Devices in the Workplace*," Ponemon Institute, February 2016, p. 1.

---

## Recommendations

1. The chief information officer should revise *Administrative Regulation 1-16* to require users to update the operating system on their mobile devices used for city business to the most current version.
2. The chief information officer should revise *Administrative Regulation 1-16* to require users to disable location services on their mobile devices used for city business when not in use.
3. The chief information officer should revise the *Administrative Regulation 1-16* to require users of all mobile devices used for city business to report lost or stolen devices to their supervisor and IT immediately.
4. The chief information officer should revise the *Administrative Regulation 1-16* to establish safeguards for safe syncing and backup of mobile devices used for city business.
5. The chief information officer should revise the *Administrative Regulation 1-16* to require encryption on all data stored on city Surface tablets.
6. The director of general services should ensure users receive mobile device security training.
7. The director of general services should implement mobile device management software on mobile devices used for city business.



---

## **Appendix A**

---

### **Director of General Services' Response**



CITY OF FOUNTAIN  
BLUFF OF THE NORTH



EMERALD CITY  
MISSOURI

# Inter-Departmental Communication

## General Services Department

**RECEIVED**

**OCT 19 2016**

**CITY AUDITOR'S OFFICE**

**Date:** October 19, 2016

**To:** Douglas Jones, City Auditor

**From:** Earnest Rouse, Assistant City Manager/General Services Director

**Subject:** Response to Performance Audit: *Mobile Device Security Risks*

Please find outlined below my responses to the recommendations contained in the Performance Audit titled above.

**Recommendation 1.** *The chief information officer should revise Administrative Regulation 1-16 to require users to update the operating system on their mobile devices used for city business to the most current version.*

**Agree.** AR 1-16 will be revised to include this recommendation and submitted to the City Manager with all updates for review and approval.

**Recommendation 2.** *The chief information officer should revise Administrative Regulation 1-16 to require users to disable location services on their mobile devices used for city business when not in use.*

**Agree.** AR 1-16 will be revised to include this recommendation and submitted to the City Manager with all updates for review and approval.

**Recommendation 3.** *The chief information officer should revise the Administrative Regulation 1-16 to require users of all mobile devices used for city business to report loss or stolen devices to their supervisor and IT immediately.*

**Agree.** AR 1-16 will be revised to include this recommendation and submitted to the City Manager with all updates for review and approval.

Douglas Jones, City Auditor  
October 19, 2016  
Page Two (2)

***Recommendation 4. The chief information officer should revise the Administrative Regulation 1-16 to establish safeguards for safe syncing and backup of mobile devices used for city business.***

Agree. AR 1-16 will be revised to include this recommendation and submitted to the City Manager with all updates for review and approval.

***Recommendation 5. The chief information officer should revise the Administrative Regulation 1-16 to require encryption on all data stored on city Surface tablets.***

Agree. AR 1-16 will be revised to include this recommendation and submitted to the City Manager with all updates for review and approval.

***Recommendation 6. The director of general services should ensure users receive mobile device security training.***

Agree. The director of general services will direct the chief information officer to identify resources needed to provide the recommended training within three (3) months of this audit response.

***Recommendation 7. The director of general services should implement mobile device management software on mobile devices used for city business.***

Agree. The director of general services will direct the chief information officer to implement mobile device management software. The chief information officer will review options, cost, and implementation time, then provide a report to the general services director within three (3) months of this audit response on the findings for this recommendation.

cc: Troy M. Schulte, City Manager  
Mary J. Miller, Chief Information Officer